AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Original) Encipher apparatus for enciphering a signal, comprising:

forming means for receiving the signal to be enciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

a plurality of encipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means; and

configuring means,

wherein each encipher functional module comprises

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and ~~le~~to produce at its corresponding parallel output a corresponding enciphered set of bits,

and each encipher functional module is operable under the control of the configuring means to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output an enciphered data block in which said respective predetermined set of bits is replaced by the corresponding enciphered set of bits produced at the parallel output of its data processing unit.

2. (Original) Encipher apparatus according to claim 1, wherein said respective data processing units are of a single type.

3. (Previously Presented) Encipher apparatus according to claim 1, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the set of bits received at its parallel input.

4. (Previously Presented) Encipher apparatus according to claim 1 wherein each of said data processing units is a reversible gate.

5. (Original) Encipher apparatus according to claim 3, wherein said reversible gate comprises a Fredkin's gate or an AND/NAND gate.

6. (Previously Presented) Encipher apparatus according to claim 1 wherein said configuring means is operative to control said encipher functional modules in accordance with a cipher design description.

7. (Original) Encipher apparatus according to claim 6, including means for receiving said cipher design description.

8. (Original) Encipher apparatus according to claim 6, including means for generating said cipher design description.

9. (Original) Encipher apparatus according to claim 8, wherein the generating means includes a random or pseudo-random number generator and is operative to use random or

pseudo-random numbers generated by said random or pseudo-random number generator to describe in code said respective predetermined sets of bits.

10. (Previously Presented) Encipher apparatus according to claim 1, wherein each of said plurality of encipher functional modules comprises a logic gate which does not conserve logic.

11. (Previously Amended) Encipher apparatus according to claim 1, wherein said plurality of encipher functional modules form a programmable circuit.

12. (Original) Encipher apparatus according to claim 11, wherein said plurality of encipher functional modules comprise a programmable logic gate array, and said configuring means comprises a programming means for programming said programmable logic gate, array.

13. (Original) Encipher apparatus according to claim 11, wherein each of said plurality of encipher functional modules comprise analogue electronic modules.

14. (Previously Presented) Encipher apparatus according to claim 1, wherein the signal is an optical signal and each of said plurality of encipher functional modules comprises optical components.

15. (Previously Presented) Encipher apparatus according to claim 1, comprising a programmable computing apparatus, wherein each of said plurality of encipher functional modules comprises a computer code routine implemented on said programmable computing apparatus.

16. (Original) Encipher apparatus according to claim 15, wherein said computer code routine is in the form of a generic module code routine repeatedly implemented dependent upon information from said configuring means.

17. (Previously Presented) Encipher apparatus according to claim 1 including first selection means for selecting a type of encipher functional module to be used from amongst a plurality of possible types of encipher functional modules, wherein said configuring means is adapted to configure the encipher apparatus to use the selected type of encipher functional module.

18. (Previously Presented) Encipher apparatus according to claim 1, including second selection means for selecting the number of said plurality of encipher functional modules to be used, wherein said configuring means is adapted to configure the encipher apparatus to use the selected number of encipher functional modules.

19. (Previously Presented) Encipher apparatus according to claim 1 including third selection means for selecting for each of said plurality of encipher functional modules the respective predetermined set of the bits of a data block received at its module input.

20. (Previously Presented) A method of enciphering a signal, the method comprising:

receiving the signal to be enciphered and forming the signal into a sequence of data blocks, each having a first predetermined number of bits;

applying the sequence of data blocks to a plurality of encipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks,

each encipher functional module comprising

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits; and

configuring each encipher functional module to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output an enciphered data block in which said respective predetermined set of bits is replaced by the corresponding enciphered set of bits produced at the parallel output of its data processing unit.

21. (Original) A method according to claim 20, wherein the encipher functional modules are of a single type.

22. (Previously Presented) A method according to claim 20, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input.

23. (Previously Amended) A method according to claim 20, wherein each of said plurality of encipher functional modules ~~each act~~acts as a reversible gate.

24. (Previously Presented) A method according to claim 20, wherein the configuring of said encipher functional modules is in accordance with a cipher design description.

25. (Original) A method according to claim 24, including receiving said cipher design description.

26. (Original) A method according to claim 24, including generating said cipher design description.

27. (Original) A method according to claim 24, including generating random or pseudo-random numbers and using the generated random or pseudo-random numbers to generate said cipher design description.

28. (Previously Presented) A method according to claim 27, wherein a respective generated random or pseudo-random number is used to describe in code the respective predetermined set of bits for a respective encipher functional module.

29. (Original) A method according to claim 28, wherein the logic operations do not conserve logic.

30. (Previously Presented) A method according to claim 20, wherein said plurality of encipher functional modules comprises a programmable logic gate array and the configuring step includes programming said programmable logic gate array.

31. (Currently Amended) A method according to claim 20, implemented by computer code on a computing apparatus, wherein each of said plurality of encipher functional modules comprises a computer code ~~routing~~routine implemented in dependence upon configuration information.

32. (Previously Presented) A method according to claim 31, wherein the computer code routine is implemented repeatedly dependent upon the number of encipher functional modules to be implemented.

33. (Previously Presented) A method according to claim 20, including selecting the type of encipher functional module to be used from amongst a plurality of possible types of encipher functional modules.

34. (Currently Amended) A method according to claim 20, including selecting the number of ~~each of~~ said plurality of encipher functional modules used.

35. (Previously Presented) A method according to claim 20, including selecting the respective predetermined set of the bits of a received data block for each of said plurality encipher functional modules.

36. (Previously Presented) Decipher apparatus for deciphering a signal, comprising:

forming means for receiving the signal to be deciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means; and

configuring means,

wherein each decipher functional module comprises

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits;

and each decipher functional module is operable under the control of the configuring means to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit.

37. (Previously Presented) Decipher apparatus according to claim 36, wherein said decipher functional modules are of a single type.

38. (Previously Presented Decipher apparatus according to claim 36, wherein said configuring means is operative to control each of said plurality decipher functional modules in accordance with a cipher design description.

39. (Original) Decipher apparatus according to claim 38, wherein said cipher design description is equivalent to the inverse of a cipher design description used to control encipher functional modules of an encipher apparatus used to produce the enciphered signal.

40. (Previously Presented) Decipher apparatus according to claim 38, including means for receiving said cipher design description.

41. (Previously Presented) Decipher apparatus according to claim 38, including means for generating said cipher design description.

42. (Original) Decipher apparatus according to claim 41, wherein the generating means includes a random or pseudo-random number generator and is operative to use random or pseudo-random numbers generated by said random or pseudo-random number generator to describe in code said respective predetermined sets of bits.

43. (Previously Presented) Decipher apparatus according to claim 36, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input.

44. (Previously Presented) Decipher apparatus according to claim 36, wherein each of said data processing units comprises a reversible gate.

45. (Original) Decipher apparatus according to claim 44, wherein said reversible gate comprises a Fredkin's gate or an AND/NAND gate.

46. (Previously Presented) Decipher apparatus according to claim 36, wherein each of said plurality of decipher functional modules comprises a logic gate which does not conserve logic.

47. (Currently Amended) Decipher apparatus according to claim 36, wherein of said plurality of decipher functional modules ~~form~~forms a programmable circuit.

48. (Original) Decipher apparatus according to claim 47, wherein said plurality of decipher functional modules comprise a programmable logic gate array, and said configuring means comprises a programming means for programming said programmable logic gate array.

49. (Previously Presented) Decipher apparatus according to claim 36, wherein the signal is an optical signal and each of said plurality of decipher functional modules comprises optical components.

50. (Currently Amended) Decipher apparatus according to claim 36, comprising a programmable computing apparatus, wherein each of said plurality of decipher functional modules comprises a computer code routine implemented on said programmable computing apparatus.

51. (Currently Amended) Decipher apparatus according to claim 50, wherein each of said plurality of decipher functional modules comprises a computer code ~~routing~~routine repeatedly implemented upon information from said configuring means.

52. (Previously Presented) Decipher apparatus according to claim 36, wherein said configuring means is responsive to type identifying information included in a cipher design description to configure the type of each of said plurality of decipher functional modules in accordance with said type identifying information.

53. (Currently Amended) Decipher apparatus according to claim 36, wherein said configuring means is responsive to module number information included in a cipher design

description to configure a corresponding number of ~~each of~~ said plurality of decipher functional modules.

54. (Previously Presented) Decipher apparatus according to claim 36, wherein said configuring means is responsive to data block size information included in a cipher design description adapted to configure the input and output of each of said plurality of decipher functional module.

55. (Previously Presented) A method of deciphering an enciphered signal, the method comprising:

receiving the signal to be deciphered and outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

applying the sequence of data blocks to a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks,

each decipher functional module comprising

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits; and

configuring each decipher functional module to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing

unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit.

56. (Original) A method according to claim 55, wherein the decipher functional modules are of a single type.

57. (Previously Presented) A method according to claim 55, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input.

58. (Currently Amended) A method according to claim 55, wherein said decipher functional modules acts as a reversible gate.

59. (Previously Presented) A method according to claim 55, wherein the configuring each of said plurality of decipher functional modules is in accordance with a cipher design description.

60. (Original) A method according to claim 59, including receiving said cipher design description.

61. (Original) A method according to claim 59, including generating said cipher design description.

62. (Original) A method according to claim 59, including generating random or pseudo-random numbers and using the generated random or pseudo-random numbers to generate said cipher design description.

63. (Original) A method according to claim 62, wherein a respective generated random or pseudo-random number is used to describe in code the respective predetermined set of bits for a respective said decipher functional module.

64. (Original) A method according to claim 63, wherein the logic operations do not conserve logic.

65. (Previously Presented) A method according to claim 55, wherein each of said plurality of decipher functional modules comprises a programmable logic gate array and the configuring step includes programming said programmable logic gate array.

66. (Previously Presented) A method according to claim 55, implemented by computer code on a computing apparatus, wherein each of said plurality of decipher functional modules comprise a computer code routine implemented in dependence upon configuration information.

67. (Original) A method according to claim 66, wherein the computer code routine is implemented repeatedly dependent upon the number of said decipher functional modules to be implemented.

68. (Previously Presented) A method according to claim 55, including selecting the type of decipher functional module to be used from amongst a plurality of possible types of decipher functional modules.

69. (Currently Amended) A method according to claim 55, including selecting the number of ~~each of~~ said plurality of decipher functional modules used.

70. (Previously Presented) A method according to claim 55, including selecting the respective predetermined set of the bits of a received data block for each of said plurality of decipher functional modules.

71-78. Cancelled.

79. (Currently Amended) Cipher apparatus comprising the encipher apparatus of claim 1 and a decipher apparatus for deciphering a signal comprising:

forming means for receiving the signal to be deciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means; and

configuring means,

wherein each decipher functional module comprises

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set

of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits, and is operable under the control of the configuring means of the decipher apparatus to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit,

wherein ~~each of said~~the plurality of ~~said~~ encipher functional modules of the encipher apparatus ~~are~~is constituted by ~~each of said~~the plurality of decipher functional modules of the decipher apparatus but are sequentially coupled in the opposite order.

80. (Currently Amended) A cipher method for enciphering and deciphering a signal comprising the encipher method of claim 20 and a decipher method comprising:

receiving the signal to be deciphered and outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

applying the sequence of data blocks to a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks, each of said plurality of ~~said~~ decipher functional module~~s~~ comprising

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set

of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits; and

configuring each of said plurality of decipher functional module to couple a response predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit..

81. (Previously Presented) Processor implemented instructions stored on a computer readable storage medium, the processor implemented instructions causing a processor to carry out the method of claim 20.

82. (Original) A carrier medium carrying the processor implementable instructions according to claim 81.

83. (Previously Presented) A storage medium storing logic to configure a programmable logic gate array to carry out the method of claim 20.